Pcap consist of an Application Program Interface for capturing network traffic, it is implemented in the libpcap library by unix-like systems.

Monitoring software may use libpcap to capture packets travelling over a network and if the versions are newer, transmit packets on a network (network link layer) and possibly get a list of network interfaces for possible use

Features

Libpcap provides packet capture filtering engines and commercial network tools like packet sniffers, network monitors, network IDS traffic generator and testers, it also supports saving captured packets to a file and reading files with the saved packets. Applications written using libpcap to capture network traffic, analyse it or read a saved capture and analyse that saved capture using the same analysis code.

Advantages

Very Easy to use

Compatible with a wide variety of programs

Can handle both incoming and outgoing data packets

Usable on both windows and Linux

Limitations

Application can read the saved file if it they can understand that format such applications are tcpdump, Wireshark

Pcap API is written in C so other languages use a wrapper to use

Does not directly support any wrappers for java, NET language or scripting language